TEST Engineering & Management

September/ October 2020
ISSN: 0193-4120 Page No. 19-24

MULTILEVEL ENCRYPTION OVER SHARED MEDIA

Anita Patil[1], Neeraj Rajput[2], Akhil Sharma[3], Ankita Shinde[4]

[1,2,3,4] Department of Information Technology, Ramrao Adik Institute of Technology, DY Patil Deemed to be University, Navi Mumbai, Nerul, Navi Mumbai, India.

Article Info
Volume 83
Page Number: 19-24
Publication Issue:
September/October 2020

Article History
Article Received*: 4 June 2020*
Revised*: 18 July 2020*
Accepted*: 20 August 2020*
Publication*: 15 September 2020*

Abstract

The Multilevel Encryption over shared media provides double security to the text message which is further encrypted in the secret image by using RSA Algorithm. The secret image is further encoded into three cover images by using Visual cryptography. The cryptographic tool which we are using for encoding the secret image into different shares is called Visual Secret Scheme. This scheme makes sure that it doesn't reveal our secret text message which is encrypted inside the secret image and further encoded into three cover images. The process of hiding a secret image into two or more images which are called shares is visual cryptography. At the receiver end, it becomes very easy for the further person to decrypt the secret image and the text information which is encrypted in the secret image by stacking the cover images together which consists of less computation. These cover images or shares encode are very safe because separately they cannot reveal anything about the secret image. In this paper generalized version of multilevel encryption over shared media is mentioned the picture to be hidden is kept under n share images and the secret text is hidden in the secret image which provides more security and prevents the image from being tampered. A simple decryption algorithm is used on the receiver end to decrypt the message. In this paper, we use the RSA algorithm which successfully encrypts a text message into the secret image and further into three cover images as chosen by the user.

1. Introduction

Multi-level encryption is a cryptographic technique of encrypting an encrypted message one or more times by using the same algorithm throughout or by using a different algorithm it can also be termed as cascade ciphering or cascade encryption. A cryptographic technique that helps in encrypting and decrypting visual information such as pictures, text, etc in a successful and efficient way is called visual cryptography. In here the concept of visual k out of n secret sharing images is established in this first the text is encrypted into a secret image and this secret image is then transformed into in shares in a way that the secret images get encrypted with these cover images on the sender side. All the receiver sides will get the three encrypted share images then these images are decrypted to get back the secret image and again the encryption is done with the help of the key to getting the original text. In traditional cryptography, the process of encryption and decryption was very time-consuming and it used to require a lot of mathematical computations. The goal was to ensure the safety of the secret images in order to do so various image secret sharing techniques are developed. The problem of using complex computation problems is being eliminated is the decryption process by using visual cryptography and hence allowing the transfer of key images in a more convenient and secure way. In techniques like Visual Cryptography Scheme or Visual secret sharing scheme, the secret image is encrypted into some power images the secret image is also called the original secret image. This gives us more clarity and the share images are also called encrypted images when various sets of cover images are stacked together it gives us the visible images which are nearly equivalent because the secret image is also called a recovered secret image. There are two different types of keys that are involved in public-key cryptography such as public key and private key. The receiver used a private key to decrypt the secret image along with the secret message and the sender uses the public key of the receiver to encrypt the secret message into the secret image. This technique provides strong security in

September/ October 2020
ISSN: 0193-4120 Page No. 19-24

various fields like Government documents, Military information, Bank Documents, Customer Identification, etc.

2. Literature Survey

	New LSB-based colour image steganography method to enhance the efficiency in payload capacity,security and integrity check, April 18	A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image , Aug 2018	A Methodology based on Steganography and Cryptography to protect highly secure messages, Feb 2019	A Steganography Scheme on JPEG Compressed Cover Image with High Embedding Capacity , Jan 2019
METHODOLOGY	Technique based on the Fisher-Yates Shuffle algorithm and 8 bpp embedding algorithm	This Steganographic method allows high capacity of data to be hidden inside the gray carrier image.	It's based on selecting a position in the color image to start hiding the secret message and matrix blocking to encrypt decrypt the holding color image.	This method is compared with some other related existing methods such as Jsteg, F5, OutGuess, Chang scheme and Lin and Liao scheme to show the effectiveness.
ADVANTAGES	• Faster and Robust • Secure	• 100% insertion of data inside the selected pixel • Simple mathematical method	• Increases security • Two private keys are used • Enhanced efficiency	• high quality reconstructed stego-image • withstand various statistical attacks
DISADVANTAGES	Not able to calculate faster size of the payload	Only used on gray scale images	• High encryption-decryption time • Low throughput	Does not survive against some statistical steganalysis like chi-square family attacks

Fig. 1. Comparative Table

2.1.1.K(n) Share

In this share, any image is taken and shared secretly. This image is encrypted employing a key given by the user. Further, the encrypted image is split into N different shares using the K N Secret Sharing Algorithm. These N shares will be distributed but, the tip user needs only K of those shares to come up with the first image. After the first image is generated it's still in encrypted form. The key which is used to encrypt the image originally is now required again to decrypt it, thus providing a further level of security.

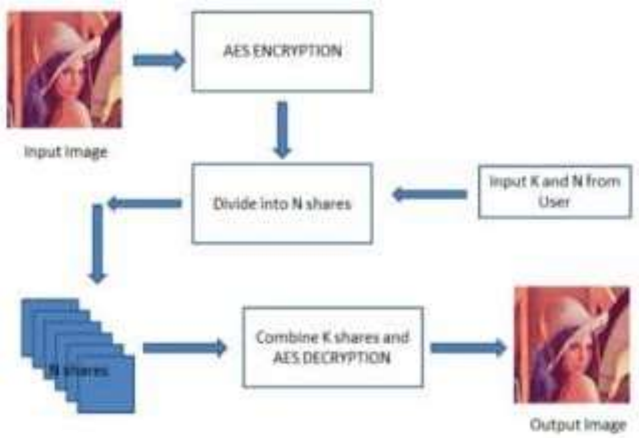

Fig. 2. Steps for K(n) Share Technique

2.1.2 VSS

The concept of Visual Secret Sharing (VSS) scheme proposed by Benny Shoar and Beruch, many of schemes are proposed to safeguard the protection of binary image. Still the issues like extensive codebook design, pixel expansion are still not being solved. This paper attempts to propose a replacement (k,n) scheme to refute the pixel expansion supported codebook and transpose of matrices. This scheme will offer promising solutions for the protection condition, computation complexity, storage requirement, fast network, and reconstructing the secret image in a more efficient and feasible manner with no distortion. In (k,n) method the concept of sharing the secret image among the n number of participants is used. Whereas there are certain conditions that need to be taken into consideration:

No participant is allowed to show the share given to a different participant. The concept behind using this scheme is that the key image is split into a different number of shares in order the , the first image is seen if any k of those cover images are been stacked together. The image will not be shown if less than the k shares are being stacked together.

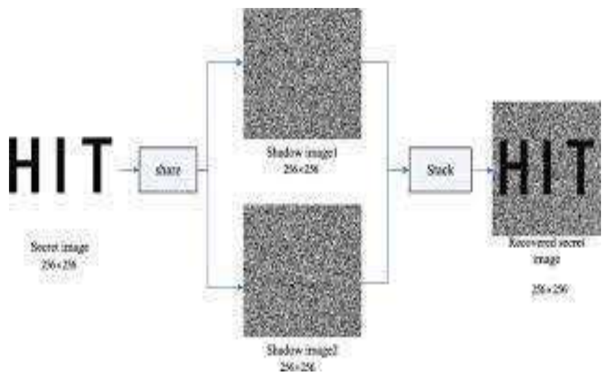

Fig. 3. VSS Technique

2.3.3 LSB (Least Significant Bit)

LSB-based steganography is used for embedding the text information in the LSB of the pixels of the cover image. It's supported the paper from the author Anil Khurana and B. Mohit Mehta.

LSB Steganography:
Step 1: Reading the shared image and text information, which has to be hidden within the shared image.
Step 2: Then convert text message in binary.
Step 3: Calculate the LSB of every pixel of the secret image. Step 4: Replacing the LSB of the

September/ October 2020
ISSN: 0193-4120 Page No. 19-24

shared image with a little bit of secret message one by one.
Step 5: Write a stego image. Algorithm to retrieve text messages:
Step 1: Reading the steganographic image.
Step 2: Calculate the LSB of every pixel of the steganographic image.
Step 3:By Retrieving bits, convert each 8 bit into character.

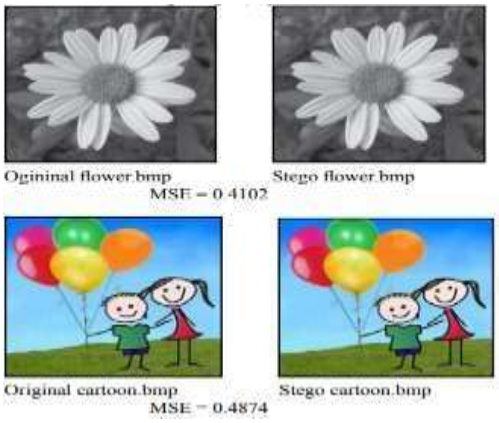

Fig. 4. LSB Steganography

2.3.4 MSB (Most Significant Bit)

MSB-based steganography embeds the text message in MSB of pixels of the secret images. It is from the paper of the author Anil Khurana and B. Mohit Mehta. The highest bit in a very series of numbers in binary in MSB.

MSB Steganography:
Step 1: Reading the secret photo and text information, which is to be hidden within the cover photo.
Step 2: Converting text information in binary.
Step 3: Calculate the MSB of every pixel of the secret photo.
Step 4: Replacing MSB of the cover photo with each little bit of secret information one by one.
Step 5: Write the steganographic photo.
The Algorithm to Retrieve Text Information:
Step 1: Reading the steganographic photo.
Step 2: Calculate the MSB of each pixel of the stego photo.
Step 3: In this step, retrieve bits and convert every 8 bits into a character that we need.

Fig. 5. MSB Steganography

2.3.5 Gray Scale Images

A grayscale image is an image where the shades of the image are only gray. The explanation for differentiating such images from the other variety of color images is that less information has to be provided for every pixel.
The smallest color depth is 8 bit (in monochrome and greyscale images) and it displays 256 different colors or reminder grey.

Fig. 6. Gray Image

3. Methodology

3.1.1 Text to Image Encryption using RSA

RSA algorithm is used to encrypt the input text into the image. In RSA, we use asymmetric cryptography. This means that there are 2 keys that are generated, one is a public key that is available to the public and between the sender and the receiver and the other is the private key which is private to the sender and the receiver. This private key must be kept secret between the sender and the receiver as it is used to decrypt the message whereas the public key is used to encrypt the message. RSA is called the one-way trap door function as there is no way to undo the encryption unless we know 'n'. The process of the public and private key, as well as the following further processes, are given as below:

a. Key generation

September/ October 2020
ISSN: 0193-4120 Page No. 19-24

The keys for the RSA algorithm are generated within the following way:
The first step is choosing of 2 distinct prime numbers p and
q. This is used to make public and private keys using the RSA function. This p and q are kept secret as it is the base to forming the RSA process. Using this p and q we compute n=p*q. The selected p and q should have the same magnitude of bits so that the resultant n is double the magnitude and a big number which is difficult to crack.
Here finding 'n' is the most difficult part as it is very difficult to get the multiplication of 2 prime numbers. Hence it becomes difficult to find n as prime factorization on n is not possible and is difficult.
Further, we use Euler's Totient function to derive the private key 'd'.
Φ (n) = (p-1) *(q-1)
Next, we choose number 'e' which is 1<e< Φ (n)
This number 'e' will be a part of our public key used during encryption process. This 'e' is relatively prime to the Totient function used. We must choose a number that has no common factors with the Totient function other than 1.
Now to finally find the private component d , we need to find the modular inverse of 'e' with respect to our Totient function Φ (n)
e*d mod(Φ (n)) = 1
Here we solve for d , which is done by the extended Euclidean Algorithm :
Extended Euclidean Algorithm is given by ax + by= gcd(a,b)
In our case we use it to find 'd':
In the equation,we substitute the values for e and Φ
(n) that we have already chosen and used e*d mod(Φ (n))=1
After this we use the Extended Euclidean Theorem to find the value of 'd' which is the private component. We find use the Euclidean Function and then use Back substitution to finally get the value of 'd'.
If the value of 'd' after back substitution comes as negative, we use the mod value to get the positive value for 'd' .

b. Key distribution
Supposed two people X and Y were to send each other secret messages. X is the sender and Y is the receiver then, Y sends its public key (e, n) which is used in the encryption process by X. It is shared through secure media and used only by X during encryption. Whereas decryption is done by Y using its private component 'd' which is never shared or transmitted to anyone.

c. Encryption
If X wants to send a message 'm' to Y then it can be done easily by making a ciphertext. The ciphertext is made using the format
CT = me mod(n)
Here this cipher text is made by using the public key (e, n) . Hence M is turned into a number and can be reversed back into the message via a padding scheme.

d. Decryption
Now Y has its private and secret component 'd' which was never shared to X . This private component is now used to decrypt the message CT to get the actual message m . This is done by the following method :
m=CTd mod(n)
Here now the initial message m sent by X is received by Y using its private key 'd' .
Here is an example of RSA encryption and decryption. The parameters used here are artificially small, but one can also use OpenSSL to generate and examine a real keypair.
Choose two distinct prime numbers, such as B .
Encoding of Image using MSB
Here we provide image security using obscurity so that no one
is aware that there is a hidden image and no one knows of its existence. We use cover images to hide the secret image. This is done on the principle that the human eye cannot detect shades that are separated by one bit.
This is done by Indexed Bitmap images. Here the size of the image increases hence it is necessary to compress the image to make it look the same.

4. Proposed System

Encryption is a process where the transformation of readable format is transformed into an unreadable format where the text is been encrypted into an image using RSA. The RSA has various functions like creating keys at the sender and the receiver part. And LSB operation on the encrypted image which has the text hidden

September/ October 2020
ISSN: 0193-4120 Page No. 19-24

as the process where the text is been transformed into the image and it cannot be visible by the human visual system as the hide of the secret image and this secret image into three cover images is done by this operation and this image is been encapsulated in such a way that is got hidden in these cover images and cannot be seen by the visual human system. As cover images can be isolated from each other and can be kept secure differently. We can retrieve the encrypted images if we stack the three-cover image this is done on the receiver side. This is decrypted using RSA for an initial text by this we get to get the initial text back at the receiver side. And hence increases the security of the secret message that we wanted to send with the help of RSA.

5. Experimental Results

The proposed algorithm is built and run-on MATLAB. The concept of multilevel encryption over shared media is modeled below it gives an overview of what we have done in our project.

Fig. 7. Text is Encrypted here.

Fig. 8. Secret Image is Encrypted in this process

Fig. 9. Secret Image is Decrypted on the receiver end.

6. Comparison between previous work and work done

Previously we saw that there have been basic methods of image steganography used which was proved beneficial but lacked the next sense of security. During this project we are using multilayer security wherein the text is first being encrypted into a secret image and further that secret image is being encoded into three cover images this makes the key information safer and robust which can't be easily tampered by an intruder. Earlier the employment of grayscale images was highly preferred because differentiating gray images from the other kind of color image is that less information has to be provided for every pixel. Whereas color images give more capacity and security. It provides a better visual quality of the stego image. Basically, the concept of using one single cover image to cover the key image is being employed in other works whereas we've used three different cover images during which the key image is being divided into K over N shares therefore the receiver's end should have the hold of all the three cover images to decrypt the key image and followed by the text which is encrypted within the secret.

7. Future Scope

There are various improvements and improvisations that can be done and can be implemented in the future. Here are some of the add- ons which can be beneficial such:

1. The encrypted three images can be shared through emails to three different people to prevent third-party attacks.

September/ October 2020
ISSN: 0193-4120 Page No. 19-24

2. Insertion of an RSA key, allows and can be connected to OTP to mail at the levels of encryption with personalized encryption process will exceed security.

8. Conclusion

In our paper, we've exhibited an encryption and decryption process of a text into an image and then this image is coded into n numbest of images supported Visual Secret Sharing Scheme. The encryption of
a text to secret photos and this is completely encrypted with the three other cover photos at the sender side. In the decryption process, this secret image from the two other cover images is first decrypted and then the secret image is decrypted into text and has been accepted. The main improvement in our paper from previous works is that we are providing multilevel encryption over shared media which ensures better security and is robust. It does not involve complex computational solving the algorithm used are RSA and Euclid's algorithm. In this, the secret text is encrypted within the secret image. Which are the first layer of encryption and further this secret image is encrypted in three cover images which provide multilevel security to the secret text due to which the intruder is unable to break through the system. The scope of the improvement during this paper lies in determining and exceeding paper goals by overcoming all the drawbacks which we hope to realize in the upcoming days.

9. References

[1] Arup Kumar Pal , Kshiramani Naik , and Rohit Agarwa," A Steganography Scheme on JPEG Compressed Cover Image with High Embedding Capacity", published by Department of Computer Science and Engineering, Indian Institute of Technology(ISM), India, January 2019.

[2] Rashad Rasras, Zaid Alqadi, Mutaz Abu Sara,
"A Methodology based on Steganography and Cryptography to protect highly secure messages", article in Engineering, Technology and Applied Science Research , February 2019.

[3] Mohammed A. Saleh, "Image Steganography Techniques ", published in College of Sciences and Arts in Ar Rass, Qassim University, Kingdom of Saudi Arabia, September 2018.

[4] Kamaldeep Joshi , Swati Gill and Rajkumar Yadav, "A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image ", In Department of Computer Science and Engineering, University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak, India,1 August 2018.

[5] Mustafa Cem Kasapbas and Wisam Elmasry, "New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check ", published in Department of Computer Engineering, Istanbul Commerce University, Istanbul, Turkey, 27 April 2018.